Amendments to the Specification:

Please replace the second full paragraph of page 3 (lines 27-32) with the amended paragraph as follows:

Therefore what is needed is a way to eliminate and avoid the bandwidth limitations on a VPN ~~cause~~ caused by the lack of preferential treatment for high-priority packets during the encryption/decryption process. What is further needed is a system and method that provides priority policies (such as QoS policies) for IPsec during the encryption and decryption process that enables a high-priority packet to be given preferential treatment over a low-priority packet during the encryption/decryption process.

Please replace the first full paragraph of page 4 (lines 4-15) with the amended paragraph as follows:

To overcome the limitations in the prior art as described above and other limitations that will become apparent upon reading and understanding the present specification, the present invention includes a system and a method for applying quality of service (QoS) policies to internet protocol security (IPsec) on a virtual private network (VPN). By using, transferring and applying the same set of policies to both network addressing and cryptographic (encryption/decryption) processing of network packets, preferential treatment of high-priority network packets are provided both during network transmission and during encryption/decryption. In particular, the present invention transfers the QoS policy model to the IPsec security program and the IPsec security program applies the QoS policies to the encryption/decryption of network packets, such that encryption/decryption can be suspended in favor of a network packet having a higher priority. Thus, the present invention allows the QoS and IPsec programs to use the same set of priority policies to give identical preferential treatment to high-priority network packets and overcome bandwidth limitations on the network.

Please replace the last paragraph of page 4 continuing as the first incomplete paragraph of page 5 (lines 29-34 of page 4 and lines 1-5 of page 5) with the amended paragraph as follows:

The method of the present invention uses the above system and includes a method of managing network packets on a computer network by applying QoS policy to IPsec programs. More specifically, the method of the present invention transmits and receives network packets over the network using QoS and QoS policies, transfers the QoS policies containing a set of regulations and criteria that determine which network packets should be given priority to the cryptographic processing, and performs cryptographic processing of the network packets in accordance with the QoS policies. The QoS policy model is applied to the cryptographic processing during both the IPsec encryption and decryption of network packets. By applying the QoS policy model to both QoS programs and IPsec programs, the flow of high-priority network packets can be optimized such that bandwidth limitations can be avoided.

Please replace the first full paragraph of page 6 (lines 3-12) with the amended paragraph as follows:

Current network packet management techniques for virtual private networks (VPN) use quality of service (QoS) programs to address outgoing network packets and internet protocol security (IPsec) to provide cryptographic processing (encryption and decryption) of network packets. The QoS programs use QoS policies that provide for preferential handling of high-priority network packets, while IPsec programs do not use these policies. One problem with this management technique, however, is that even though QoS ~~give~~ gives preferential treatment to high-priority network packets during transmission and reception of the packets on the network, during encryption and decryption of network packets under IPsec, these same high priority packets are not given preferential treatment and all packets are treated as equal.

Please replace the first full paragraph of page 6 (lines 3-12) with the amended paragraph as follows:

The network packet having the highest priority is selected and cryptographic processing is begun on this network packet (box 430). Meanwhile, the present invention checks to determine whether any network packets having a higher priority than the current network packet being processed have arrived for processing (box 440). If not, then the present invention continues processing of the current network packet (box 450). Otherwise, processing of the current network packets is suspended in favor of the higher priority network packet that was recently received (box 460). Thus, current processing of any lower-priority network packet whenever a higher-priority network packet is received is performed for cryptographic processing. In this way, the present invention ensures that high-priority network packets are not significantly slowed down during the encryption/decryption processing.